Supplier Security Standard

Effective Date: January 2024

Table of Contents

1.0 Introduction and Purpose

New York Life has developed this Supplier Security Standard (the "**Standard**") to ensure Suppliers protect and maintain the Confidentiality, Integrity, and Availability of Scoped IT Assets. Capitalized terms used in this Standard have the meanings specified in their immediate context, or in Section 6.0 (Glossary), in the Agreement, or in the Supplemental Glossary for Supplier Security Standard (in descending order of precedence).

This Standard provides the minimum control requirements that all Suppliers must adopt to ensure that Scoped IT Assets are protected from loss, misappropriation, mishandling, alteration or other damage. New York Life recognizes that there may be multiple approaches to accomplish a particular minimum control requirement. These minimum control requirements are not intended to replace Supplier's standard policies and procedures but are intended to address the minimum controls that Supplier must have in place as part of Supplier's standard policies and procedures. As technology trends change, Supplier should ensure they are adhering to these minimum control requirements as it relates to any new and emerging technologies. Supplier must document in reasonable detail how a particular control meets the stated minimum control requirement. Not all of the stated minimum control requirements will apply to all Services or other deliverables, but Supplier must be able to reasonably show how the minimum control requirement does not apply. These minimum control requirements do not limit Supplier's obligations under the Agreement or applicable Law.

Suppliers providing Hosted Solutions and Service Delivery Center (SDC) services must also fully comply with Sections 3 and 4 (Hosted Solutions Requirements and Service Delivery Center Security Requirements, respectively) of this Standard. In the event of any conflict between the general requirements of this Standard and the Hosted Solutions or SDC requirements, Hosted Solutions and SDC Suppliers will comply with the more stringent requirements.

Supplier's failure to meet this Standard may expose New York Life, its employees, customers, and business partners to risk, and may result in harm to New York Life including financial loss, service disruptions, regulatory sanctions, and reputational damage. New York Life requires all Suppliers, including Supplier Personnel and Subcontractors, who are engaged in the provision of products and services to New York Life or who otherwise manage, operate, interact with, or have access to Scoped IT Assets, to meet this Standard[1].

This Standard supplements: (1) the Agreement, and (2) additional New York Life policies and standards. If there are conflicts or inconsistencies among this Standard, the Agreement, or another New York Life policy or standard, New York Life expects Supplier to comply with the terms that provide the greatest level of protection for New York Life and its Scoped IT Assets.

Note: Insurance-Related Servicers are covered by requirements defined in the New York Life Insurance-Related Servicers Security Standard.

[1] Issue Management of Non-Compliance to Policy and Standards: It is the responsibility of the applicable NYL Business Unit engaging with a supplier to ensure compliance with this standard and, if applicable, for meeting the requirements as stated in the Issues Management Standard for any non-compliance with policies and standards or any issue identified that poses an increased level of risk to New York Life.

2.0 Supplier Security Requirements

2.1 Comprehensive Security Program & Practices

2.1.1 Supplier must adopt, implement, maintain, review, and adhere to a comprehensive written security program designed to protect the Confidentiality, Integrity, and Availability of Scoped IT Assets.

2.1.2 Supplier must perform annual risk assessments that include (1) identification of all Scoped IT Assets, (2) criticality and sensitivity of each Scoped IT Asset, (3) extent to which Supplier must use or access each Scoped IT Asset in the performance of its obligations to New York Life, (4) assessment of all controls related to Supplier's security program, and (5) requirements from industry standards and frameworks.

2.1.3 At a minimum, Supplier's security program must address the following areas (as applicable to the Scoped IT Assets and to Supplier's obligations to New York Life):

1. Data governance, classification and protection;
2. Management of Records and non-records;
3. Access Controls and identity management;
4. Business continuity and disaster recovery planning;
5. Capacity and performance planning;
6. Systems operations and Availability concerns and related elements such as network security, network monitoring, and defensive measures;
7. Vulnerability Management;
8. Physical security and environmental controls;
9. Customer data privacy;
10. Vendor and third-party service provider risk management;
11. Asset inventory and device management;
12. Systems and application development and quality assurance;
13. Security Event response processes and procedures;
14. Acceptable use and clean workspace; and
15. Documented and distributed disciplinary policy for violation of security program.

2.1.4 The Supplier's security program must be approved by a senior officer of Supplier (e.g., a C-level executive or his or her direct report) who has oversight of cybersecurity.

2.1.5 Supplier must provide written notice to New York Life (as specified in the Agreement) before Supplier makes any changes to the Supplier's security program

that reduce or otherwise degrade the requirements or obligations of Supplier's security program.

2.2 Supplier Personnel

2.2.1 Supplier must ensure that its security program (including its cyber security and privacy policies) is published, updated annually and effectively communicated to all Supplier Personnel. Supplier must develop, document, and maintain security awareness, education, and other training to ensure that all Supplier Personnel fully understand their individual responsibilities and corporate security mandates, including Supplier's security program.

2.2.2 Supplier must ensure that all Supplier Personnel have certified in writing that they have reviewed and will comply with Supplier's security program, specifically those components that relate to Supplier's customers and those customer's data (in the case of New York Life as customer, the Scoped IT Assets).

2.2.3 Except as prohibited under Applicable Law, Supplier will ensure that Supplier Personnel who are assigned to perform work or will have access to NYL Systems do not perform any of their professional responsibilities while impaired or otherwise under the influence of illegal drugs or of improperly used legal drugs or alcohol. If Supplier becomes aware that any Supplier Personnel has performed, is performing, or is likely to perform his or her duties while impaired or otherwise under the influence, Supplier will immediately stop those Supplier Personnel from performing duties for NYL, remove those Supplier Personnel from the NYL account, and initiate the termination of their access to NYL Systems.

2.2.4 Supplier will initiate and conduct background and criminal checks of each Supplier Personnel intended to perform work as part of the services Supplier provides to New York Life, no more than three years prior to the assignment start date, and then only after informing the candidate of its intent and securing permission to run a background check. Supplier will conduct all background checks at its own expense, consistent with criteria provided or approved in advance by NYL, and in accordance with Applicable Law of the locations where such individuals work. Supplier will not assign to NYL, or retain on assignment to provide Services to NYL, any Supplier Personnel who did not successfully pass the background check or who Supplier knows, suspects, or has reason to believe has been convicted of, pled guilty to, or participated in a pretrial diversion for, a crime involving dishonesty, breach of trust, money laundering, or any other similar type of crime. The criminal check components must be reperformed at each annual anniversary of the Agreement Effective Date for Supplier Personnel who (1) have ongoing and independent access to NYL Systems (i.e., Supplier Personnel is issued log on credentials), (2) require access to or use of Personal Data to perform Supplier's obligations, or (3) have unescorted or independent access to NYL's premises (i.e., issued a NYL Badge).

2.2.5 Upon NYL's request, Supplier will provide written evidence that the checks specified in Sections 2.23 (Non-Impairment) and 2.2.4 (Background Checks) have been performed.

2.2.6 Supplier must employ or retain Supplier Personnel as needed to effectively manage Supplier's security risks (cyber or otherwise) and to perform core cyber security functions.

2.2.7 Supplier must provide for and require Supplier Personnel engaged in performing cybersecurity functions to attend regular cybersecurity updates and training sessions aligned to prevailing standards for the financial services and insurance industries.

2.2.8 Supplier must ensure that departing or terminated Supplier Personnel return (1) all Scoped IT Assets to Supplier on or before Supplier Personnel's last day of employment with Supplier, and (2) all New York Life Data on or before the last day on assignment to New York Life. As part of its documented processes for the termination or departure of Supplier Personnel, or cessation of services by Supplier Personnel to New York Life, immediately following termination or departure of Supplier Personnel, or cessation of services, that required access to Scoped IT Assets, Supplier must (1) cancel/remove such Supplier Personnel's access to Scoped IT Assets, including revocation of access to Supplier Systems and New York Life Data, and (2) notify New York Life of the name of impacted Supplier Personnel.

In addition, to the extent that Supplier has staff dedicated to NYL services, Supplier must maintain a list of Supplier Personnel who are no longer assigned to New York Life services and must provide that list to New York Life on a monthly basis.

2.2.9 Supplier must ensure there is no sharing of tokens, user IDs, passwords or any other similar information with and between any persons (including with and between Supplier Personnel) under any circumstances. Appropriate auditable break-glass procedures must be in place for New York Life approved emergency accounts.

2.3 Duty of Care & Use Restrictions

2.3.1 Without limiting its other obligations to New York Life, Supplier must adopt, maintain, review and adhere to risk-based security practices and procedures to safeguard Scoped IT Assets from anticipated threats or hazards to Confidentiality, Integrity, and Availability.

2.3.2 Supplier must recertify account access privileges and roles for Scoped IT Assets at least annually for non-privileged accounts, and quarterly for privileged (access to process High Risk Transactions and system administrative access) accounts, or at a lesser frequency as approved in writing by New York Life.

2.3.3 Supplier must provide New York Life with the list of Supplier Personnel who have access to Scoped IT Assets and other required data fields to support New York Life's recertification process.

2.4 Return/Destruction/Maintenance of Scoped IT Assets

2.4.1 Supplier must develop, implement, maintain, review and monitor ownership, inventory, return, and acceptable uses of Scoped IT Assets.

2.4.2 Supplier must develop, implement, maintain, and monitor procedures and controls for the secure handling, transfer, destruction, and disposal of Scoped IT Assets in any form.

2.4.3 Supplier must obtain written approval from New York Life before allowing Supplier Personnel to access Scoped IT Assets through personal devices. Notwithstanding the foregoing, any personal devices used to access Scoped IT Assets, whether approved or not, are deemed to be part of Supplier Systems.

2.4.4 Supplier must dispose of Scoped IT Assets in a way so that it may not be decoded, read, accessed, or decompiled.

2.4.5 Supplier must have the ability to comply with New York Life Records management requirements (as communicated to Supplier) including Hold Orders, searches, retrievals, and timely destruction.

2.4.6 Supplier will destroy any retained New York Life Data as soon as its retention obligations have been met, unless a Hold Order is in place, and will provide a Certification of Destruction (COD) to New York Life. The following information should be included on the COD:

1. Attestation that New York Life Data was deleted/destroyed;
2. Identify/describe the New York Life Data that was destroyed;
3. The date range of the deletion period;
4. Volume of New York Life Data;
5. Method of deletion and a statement that the method complies with all Applicable Laws and any contractual requirements; and
6. Any issues and their resolution should be described; and
7. The name, signature and contact information of Supplier Personnel who executes the process or have oversight responsibility of the deletion/destruction process.

2.5 Physical Security

2.5.1 Supplier must maintain all Scoped IT Assets in secure facilities owned, operated, or contracted by Supplier or in similarly secure manner for portable Scoped IT Assets e.g., laptop computers, removable media, or mobile devices.

2.5.2 Supplier must limit access to and within its facilities to those Supplier Personnel with job-related needs and appropriate authorization.

2.5.3 Supplier must monitor access to its facilities using measures that may include, by example and not limitation, security guards, CCTV surveillance cameras placed to monitor entry and exit points, and authorized entry systems requiring badge access or similar methods capable of recording entry and exit information, consistent with Supplier's risk assessment. Logs detailing facilities access must be stored for a minimum period of three (3) years, and CCTV video surveillance data must be retained for minimum of ninety (90) days. Once the retention period has been met, the content should be properly deleted and/or destroyed (unless subject to a Hold Order).

2.5.4 Supplier must maintain environmental controls at all facilities hosting Scoped IT Assets. The environmental controls may include, by example and not limitation, climate control (temperature and humidity), raised floor, smoke detector, heat detector, fluid sensor, fire suppression, uninterrupted power supply including backup generators, and fire extinguisher equipment.

2.5.5 Use of any camera to capture New York Life Data on personal devices by Supplier Personnel is prohibited.

2.5.6 Supplier must maintain all backup and archival media related to Scoped IT Assets in secure, environmentally-controlled storage areas owned, operated, or contracted for by Supplier in accordance with New York Life's retention instructions.

2.5.7 Supplier must ensure Remote Work (from outside Supplier's office and facilities) is prohibited for employees with remote access to New York Life Data unless approved in advance and in writing by New York Life. Approvals must be maintained and made available for both Supplier and New York Life audits. Supplier must implement and monitor security controls for Remote Work in accordance with Section 5.0.

2.6 Network & Communications Security

2.6.1 Supplier must deploy multiple layers of defense on Supplier Systems, including but not limited to firewalls, Intrusion Prevention Systems (IPS), and Intrusion Detection Systems (IDS), consistent with Supplier's risk assessment. Supplier must also actively monitor Supplier Systems consistent with its risk assessment.

2.6.2 Supplier must configure network-related components of Supplier Systems (e.g. firewalls, network routers, switches, load balancers, domain name servers, mail servers, AWS, Azure, etc.) in accordance with its risk assessment and generally accepted information security standards in Supplier's industry and the insurance, investment, and financial services industries.

2.6.3 Supplier must logically segregate Supplier's network and implement a Demilitarized Zone (DMZ) to house all Internet facing infrastructure, and to provide separation between the Internet and Supplier's internal network. Additionally, the internal wireless and guest wireless networks must be segregated (i.e. via firewalls) from the rest of the Supplier's network and must be encrypted per the Approved Encryption.

2.6.4 Supplier must review at least annually Firewall and router rule-sets and configurations to clean up any unneeded, outdated, or incorrect rules, and to ensure that all rule sets allow only authorized services and ports that match the documented business justifications.

2.6.5 Supplier must specifically deny all inbound and outbound traffic by using "deny all" rule statements, and explicitly allow only authorized traffic (with rules based on target and source destinations, network services, protocols and ports).

2.6.6 Supplier must have a process to identify, review, and approve access to external non-job related or black-listed websites (e.g. terrorism, hacking sites, third-party document repository sites, public email and IM, and social media).

2.7 Infrastructure/Platforms/Services/Desktop/Operations Security

2.7.1 Supplier must configure all infrastructure, platforms, and services (e.g., operating systems, web servers, database servers, firewalls, routers) in accordance with its risk assessment and generally accepted information security standards in Supplier's industry and the insurance, investment, and financial services industries.

2.7.2 Where encryption keys are used, Supplier must have and administer a documented and approved key management process that addresses all phases of key lifecycle management, including but not limited to key creation, key use, key storage, key recovery, key revocation, and key destruction.

2.7.3 Supplier must ensure that all remote access to Scoped IT Assets is performed over encrypted connections (e.g. SSH, SCP, SSL-enabled web management interfaces, and VPN/VDI solutions), utilizing the applicable Approved Encryption.

2.7.4 Supplier must implement desktop controls that include, by example and not limitation: (1) restricting End Users from being granted local administrator-level privileges, (2) disabling key desktop settings (e.g. screen saver, anti-virus) so that End User cannot alter those settings, (3) prohibiting and preventing New York Life Data from being stored on the local desktop, and (4) blocking peripheral devices (e.g., CD, DVD, USB drives).

2.7.5 Supplier must use Risk-Based Authentication when granting access to Scoped IT Assets not originating within Supplier Systems.

2.7.6 Supplier must use Multi-Factor Authentication for any access to Scoped IT Assets (including its accounts on Amazon Web Services (AWS), Microsoft Azure, and other cloud service providers) not originating within Supplier Systems.

2.7.7 All New York Life Data, including backup and archive copies, must be encrypted using Approved Encryption.

2.7.8 Supplier must perform periodic backup data restoration tests and data integrity tests from backup media to ensure backup data can be recovered.

2.7.9 All New York Life Data must be encrypted in transit using Approved Encryption.

2.7.10 Supplier must ensure that any changes to Supplier Systems are documented via formal change management procedures. Supplier must provide separate development, test, and production environments within Supplier Systems. Changes must be fully validated in one environment before being migrated to the next higher environment.

2.7.11 Supplier must ensure that all system clocks for Supplier Systems are synchronized with a single reference time source.

2.7.12 Supplier must maintain access, activity, and audit logs for changes to Supplier infrastructure/platforms/services, including tracking of both access attempts and privileged access to Scoped IT Assets, in accordance with New York Life's retention instructions and Applicable Law.

2.7.13 Supplier must use commercially reasonable efforts to monitor, on a regular basis system performance, reputable sources of security Vulnerability information (FIRST or CERT/CC) and incident tickets. Supplier must timely develop and issue patches for its proprietary products and deploy patches for third-party components of Supplier Systems as provided by the third-party provider, to correct problems, improve performance, and enhance security of Supplier Systems.

2.7.14 Supplier must implement, for Scoped IT Assets, time out and termination of system communication sessions and security sessions or contexts after a twenty (20) minute (or less as mutually agreed upon) period of user inactivity.

2.7.15 Supplier must not use production data for testing in non-production environment(s) except as authorized by New York Life.

2.7.16 Supplier must define and document a mobile device security policy including the following specifications:

1. Restrict Supplier Personnel access to New York Life Data on mobile devices;
2. Mandate encryption of all New York Life Data stored on the device; and
3. Require the use of central mobile device management software (with remote wipe functionality, malware detection), and require other security controls to best protect New York Life Data.

2.7.17 Supplier must monitor on a daily basis scheduled jobs (e.g., batch processing, backups, data feeds, etc.), to ensure their successful completion. Job failures must be logged, reviewed and remediated in a timely manner.

2.8 Additional Software Provisions

For additional requirements associated with hosted solutions refer to Section 3.0.

2.8.1 Supplier must ensure, all software provided to New York Life (or otherwise leveraged or utilized by Supplier in the provision of products and services to New York Life) is not susceptible to the most recently published OWASP top 10 vulnerabilities (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project). At New York Life's request, Supplier will provide written certification of its compliance with these requirements, which written certification must include confirmation by Supplier that, on an annual basis, as well as upon issuance of a major upgrade, Supplier, directly or via a qualified third party, conducted a static and dynamic code/program analysis, and penetration testing that confirmed the absence of any bugs or flaws, including by way of example and not limitation, buffer overflows/underflows, NULL pointer dereferences, resource leaks, or any other reliability or security problem.

2.8.2 Supplier must, when possible, keep information in session and avoid using web browser cookies, however, if web browser cookies cannot be avoided, ensure that web browser cookies containing New York Life Data or information that should not be altered outside of the Hosted Solution are encrypted using Approved Encryption (which Approved Encryption is independent from any transport encryption such as Secure Socket Layer); all other cookies must be opaque.

2.8.3 When integrating with New York Life systems or applications via Application Programming Interfaces (APIs), Supplier must work with New York Life system architecture subject-matter-experts to review and obtain approval for proposed API implementation.

2.8.4 Supplier must have a documented Secure Software Development Life Cycle (SSDLC) for the purpose of defining, acquiring, developing, enhancing, modifying, testing or implementing Supplier System, that will be shared with NYL on written request.

2.8.5 Supplier must be able to document adherence to their SSDLC, and upon request supply evidence of adherence.

2.8.6 For software deliverables being developed by Supplier for New York Life, Supplier must adhere to the following:

1. Adhere to the New York Life Technology Delivery Lifecycle (TDLC) standards and artifact requirements.
2. To the extent that the New York Life TDLC does not address a particular issue or cannot be followed without material additional effort or expense, provide a documented Secure Software Development Life Cycle (SSDLC) and proof of adherence to the SSDLC.
3. Provide a written set of security requirements and coding guidelines to New York Life that indicate how developed code will be created, formatted, structured, tested and commented by Supplier.

4. Ensure that all developed code is reviewed and validated using a documented process, developed code is then tested against the security requirements and coding guidelines before Supplier provides the software deliverable to New York Life for any additional testing or review.
5. Identify the key risks to other Scoped IT Assets arising through the intended operation of the software, including risks to their Confidentiality, Availability, Integrity and Accountability, and develop appropriate controls to mitigate or minimize those risks.
6. Conduct an analysis of the CWE/SANS Top 25 Most Dangerous Software Errors or most common programming errors and provide New York Life with written documentation evidencing that any such errors have been fully mitigated and resolved.
7. Privileged accounts are documented.

2.9 Identity and Access Management

2.9.1 Supplier must ensure End User access capabilities for Scoped IT Assets are granted on a need-to-know basis.

1. Privileges must be consistent with assigned job responsibilities and must be configured with Least Privilege.
2. Supplier must clearly define the extent to which administrative or super user accounts may have access to Scoped IT Assets and the security controls in place to prevent misuse.

2.9.2 Supplier must implement Access Controls designed to protect Scoped IT Assets from compromise. Protections must include but are not limited to appropriate authorization and management of all Scoped IT Assets.

2.9.3 Supplier must have a process workflow in place, including an approval process, to request, change, and remove End User access to Scoped IT Assets in a timely manner.

2.9.4 Supplier must obtain New York Life authorization to manage authentication, authorization or identities, for all Supplier Personnel that require access to Scoped IT Assets, and for New York Life access to Supplier's systems (when it's not feasible to integrate with New York Life's authentication mechanisms). Supplier must maintain and adhere to procedures that restrict End User access to information and application functions and prevent and detect unauthorized access to Scoped IT Assets. At a minimum, Supplier must have a formal password policy, for Supplier Personnel and for New York Life access to Supplier's systems (when it's not feasible to integrate with New York Life's authentication mechanisms) that includes the following controls:

1. Default authentication information (user accounts and passwords) is removed or disabled upon installation of new system or software;

2. Initial passwords provided to users are temporary, unique and require change on first use;
3. User's identity is validated prior to performing password resets or communicating passwords;
4. Passwords are never transmitted or stored in clear text but protected using Approved Encryption;
5. Password management systems do not display passwords on screen in plain text;
6. Minimum password length and complexity requirements are enforced;
7. Users are forced to change passwords after a predefined timeframe; and
8. User account lockout after 10 or less consecutive failed login attempts.
9. All passwords must be encrypted/hashed using Approved Encryption when stored and in transit.
10. Password files must be stored separately from the application system data.

2.9.5 For Supplier-developed software deployed on New York Life's private network and for Hosted software:

1. All End User identities must be managed by New York Life within the New York Life Corporate Directory.
2. All authentications of End User identities must be done via a New York Life approved method (currently AD/LDAP/OpenID, OAUTH 2.0 or SAML 2.0), as determined during the software requirements and design phase.
3. All End User authorization must take place through a New York Life approved platform (currently Directory, ACF2, and home grown).

2.9.6 Supplier must employ multi-layered controls to protect New York Life and its clients from unauthorized access to Scoped IT Assets. These controls must include an authentication protocol governing the requirements for End Users to access Scoped IT Assets, as well as additional fraud prevention controls to prevent unauthorized access such as disbursement limits, guidelines around High Risk Transactions (as defined by New York Life), and fraud monitoring.

2.10 Log Files

2.10.1 Supplier must adopt procedures and implement systems to track and maintain all Records, data, and schedules that allow for the complete and accurate reconstruction of all financial transactions for at least the past eight (8) years (or longer as may be required by New York Life's retention instructions, Applicable Law, or the Agreement) to support normal operations. Once the retention period has been met, the content should be properly destroyed, (unless subject to a Hold Order)

2.10.2 Supplier must maintain, for a period of at least three (3) years (or longer as may be required by New York Life's retention instructions, Applicable Law, or the

Agreement), detailed log files (for audit trail) concerning all activity on Scoped IT Assets, to enable Supplier to detect and respond to a Security Event. At a minimum, the following logs must be available in a machine-readable format, and protected against unauthorized access, modification, or deletion:

1. All End User sessions established, including user ID and date/time of authentication;
2. Roles assigned to the user ID within solution at any point in time;
3. Actions performed using the user ID when accessing the Scoped IT Asset;
4. Information related to the reception of specific information from an End User or from another system;
5. Failed authentication attempts for End Users;
6. Unauthorized attempts to access the Scoped IT Asset in whole or in part;
7. Administrator and operator actions;
8. Events generated (e.g., commands issued) to make changes in security profiles, permission levels, application security configurations, and/or system resources; and
9. Provisioning and deprovisioning of End Users and Scoped IT Assets.

2.11 Vulnerability Assessment and Penetration Testing

2.11.1 Supplier must test the implementation of its information security measures (including Supplier's security program) as applied to its Scoped IT Assets through the use of Vulnerability scanning tools and penetration testing, including monitoring, periodic penetration testing (which may include phishing and social engineering campaigns), and Vulnerability assessments.

2.11.2 Vulnerability Assessment

1. At least bi-annually, Supplier must conduct a Vulnerability assessment by running authenticated scans from a scanning tool against Supplier Systems.
2. Supplier must mitigate all critical/very high/high vulnerabilities (e.g., as defined in CVE or similar assessment standards) identified during the Vulnerability assessment by working diligently and continuously after learning of the Vulnerability until the Vulnerability has been remediated (which remediation will not exceed 30-days unless such longer period of time has been approved in writing by New York Life). Moderate rated vulnerabilities within 90 days, and lower rated vulnerabilities in accordance with Supplier's internal policies and standards.
3. To the extent Supplier has identified areas, processes, or elements of or related to Supplier Systems that require material improvement, updating or redesign, Supplier must document the identification and the remedial efforts planned and underway to address such items. Summary documentation of these plans must be available for inspection by New York Life.

2.11.3 Penetration Testing

1. At least annually, Supplier must perform penetration tests on internet-facing Supplier Systems.
2. Vulnerabilities identified should be addressed in alignment with Section 2.11.2.2
3. Supplier must share summary results of risk ranked Vulnerability status with New York Life on request.

2.12 Audits and Verification

2.12.1 In addition to any audit requirements in the Agreement, Supplier will cause an annual audit of the design, suitability, and operating effectiveness of controls relating to availability, security, processing integrity, confidentiality, and privacy, or an audit based on ISO 27001:2013 (or any successor information security standards) including substantive review of the effectiveness of Supplier's controls, to be performed on Scoped IT Assets and provide to NYL a copy of each resulting report (e.g. SOC 2 Type II).

2.12.2 Supplier must permit representatives of New York Life, with prior notice and at reasonable times, to examine and verify compliance with Supplier's obligations with respect to the safeguarding and use of Scoped IT Assets, and the detection, prevention, and mitigation of an actual or attempted theft or misappropriation of computing resources and New York Life Data. Additionally, in the event of a Security Event, New York Life may perform immediate audits and reviews of the affected Scoped IT Assets. Any such examination, verification, audit and review may include:

1. Onsite security and remote desk-based audits and reviews,
2. Security assessments requiring responses from Supplier or its Personnel,
3. Visits to locations where New York Life Data may be stored, processed, administered or otherwise accessed, and
4. Review of all Records, files and systems in Supplier's or Supplier Personnel's possession relating to New York Life.

2.13 Business Continuity and Disaster Recovery Plans

2.13.1 Supplier must conduct periodic Business Impact Analysis (BIA) and/or Risk Assessments designed to identify and prioritize critical business functions, processes, dependencies and estimated impact of downtime in line with financial services and insurance industries best practices and regulations.

2.13.2 Supplier must have business continuity and disaster recovery plans that are designed to satisfy and comply with this standard and internationally accepted IT recovery planning standards, and that ensure the operational resiliency needs of New York Life. Supplier Systems will include redundancy for all major system components, where appropriate.

2.13.3 Supplier must ensure Business Continuity and/or Disaster Recovery plan includes processes and procedures for resuming operations promptly and within the

contractually agreed upon recovery time. Without limiting the foregoing, Supplier's Business Continuity and Disaster Recovery plan will require Supplier at a minimum to:

1. perform backups as appropriate to maximize Availability of the services in circumstances where Supplier invokes its Business Continuity or Disaster Recovery plan;
2. include procedures and any third-party agreements for replacement equipment, telecommunications capabilities, and off-site production and disaster recovery facilities;
3. store back-up media to a secondary or alternate location that is geographically distant from the Supplier's primary location(s);
4. maintain and use redundant communications lines and servers that will facilitate NYL's access to the hot site or any other remote facility used by Supplier during a disaster;
5. develop and maintain plans for the transition back from the disaster recovery site to Supplier facilities for the affected services and restoration of services at the original site when feasible; and
6. coordinate the recovery plan and its operations with NYL's own recovery plans, including with testing of NYL's plans.

2.13.4 Supplier must design and test its Disaster Recovery plan including Data Center Recovery Exercises at least annually or as required by State or Federal regulatory guidelines for all business areas. Any deviation from the Recovery Time Objective (RTO) approved by New York Life must demonstrate successful remediation within 90 days or an exception must be filed.

2.13.5 Supplier must ensure business continuity and disaster recovery plans receive senior or executive level management approval on an annual basis, or as material changes occur. Material changes may include any major updates that review people, process, and technology related mission critical deliverables.

2.13.6 Supplier must provide New York Life (upon request) a copy of the most recent business continuity and/or disaster recovery test summary report which shall include at a minimum of the test scope, success criteria, tests performed, and test results including identified risks and remediation plan.

2.13.7 Supplier must immediately notify New York Life of any event that is or could potentially be disruptive or impact the delivery of product and services by Supplier to New York Life. Supplier must notify New York Life of the status of actual and potential events and impacts of such events from the beginning of an event through closure.

2.13.8 Supplier must periodically validate that the Cyber Security protection measures in place within the disaster recovery environment are equivalent to those in production environment.

2.13.9 Supplier must ensure that the disaster recovery network environment (i.e. hardware and software) is maintained in synch with the production environment.

3.0 Additional Hosted Services Requirements

In addition to the general requirements set forth in in Section 2.0 of this Standard, Hosted Services providers must also be fully compliant with the following Hosted Services security requirements. If there is a conflict between a general requirement and these Hosted Services security requirements, Supplier will comply with the more stringent requirement.

3.1 Comprehensive Security Program & Practices

3.1.1 Supplier must ensure that safeguards are implemented in its environment (based on policies and procedures, business critical assets and/or sensitive user data, and compliance with legal, statutory, and regulatory compliance obligations) to ensure that New York Life Data is properly segregated and only accessible by authorized users.

3.1.2 Supplier must maintain an inventory of New York Life Data, and document data flows across servers, databases, and network infrastructure (including geographic locations of all infrastructure).

3.2 Network and Communication Security

3.2.1 Supplier must ensure IP address and location filtering are used to authenticate connections from specific locations and equipment. Adequate controls must be in place to prevent the connection of unauthorized devices to New York Life applications and data.

3.2.2 Supplier must, at the request of New York Life, restrict access to any component(s) of the networks, systems, services, and applications used to provide products/services to New York Life.

3.3 Infrastructure/Platforms/Services/Desktop/Operations Security

3.3.1 Supplier must provide New York Life with written security configuration guidelines that fully describe all relevant configuration options for relevant software and the implications for the overall security of the software. These guidelines must include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how all should be configured for optimal security. The default configuration for the software must be set at highest security level.

3.3.2 Supplier must ensure all New York Life Data can be exported, upon request by New York Life, in an industry-standard format generally accepted in the financial services and insurance industries (e.g. JSON, XML and CSV).

3.4 Identity and Access Management

3.4.1 Supplier must make the following available on request for all New York Life identities used in any Hosted Solutions: ID, last login, roles assigned to the ID within the Hosted Solution (i.e., administrator, read-only, etc.), and which Hosted Solutions have been accessed using the ID.

3.4.2 Supplier must ensure hosted solutions are secured using a web-based single sign-on (SSO) method accepted and approved (in advance and in writing) by New York Life (currently SAML 2.0 identity federation standards where New York Life has the identity provider role).

3.4.3 Supplier must, in advance of production deployment, use a New York Life approved non-SSO method. Non-SSO methods must, at a minimum, enforce a password policy meeting New York Life standards.

4.0 Additional Service Delivery Center (SDC) Security Requirements

SDC security requirements have two tiers: Non-Dedicated and Dedicated facilities. These security requirements will be applied as described below.

Non-Dedicated SDC

In addition to the requirements in Sections 2 and 3 above, SDC Suppliers must be fully compliant with the following SDC security requirements.

4.1 Comprehensive Security Program & Practices

4.1.1 Supplier must identify a named full-time Supplier employee responsible for monitoring and reporting non-compliance with the New York Life requirements.

4.2 Supplier Personnel

4.2.1 Supplier will ensure that it provides security training to all Supplier Personnel who will be assigned to New York Life in advance of Supplier Personnel assignment start date. Security training will include, but not be limited to role-based security awareness, protection of information, security expectations per supplier policies and New York Life Supplier Security Standard. Supplier will maintain a record of all Supplier Personnel that have attended security training and will make this information available to New York Life upon request.

4.3 Audits and Verification

4.3.1 In addition to any audit provisions in the Agreement with New York Life or in New York Life Policies, Supplier will allow New York Life to perform onsite audits and reviews on an annual basis to verify Supplier's compliance with this Standard. Any

exceptions to the Standard must be approved in writing by authorized New York Life personnel.

4.4 Business Continuity, Disaster Recovery and Resiliency Plan

4.4.1 Supplier must perform a worksite recovery and/or tabletop exercise that simulate real events that would disrupt operations to New York Life at least annually to ensure plans remain viable and executable.

Dedicated SDC

In addition to the requirements within the Non-Dedicated SDC Section, SDC Suppliers in this tier must be fully compliant with the following SDC security requirements.

4.5 Physical Security

4.5.1 Supplier must ensure all SDC technology infrastructure (e.g. servers & network equipment) is dedicated to New York Life; is caged and locked; is distinct and segregated from co-tenants and is subject to a formal documented auditable process to ensure appropriate management of access.

4.5.2 Supplier must maintain an access register for all persons entering the SDC, which will include, but not be limited to, date, time, name, and purpose.

4.5.3 Supplier must ensure all New York Life project activities are carried out in a secure and dedicated area of the SDC accessed only by Supplier Personnel dedicated to providing services to New York Life and fully segregated from co-tenants and unauthorized personnel.

4.5.4 Supplier must ensure all entrances to the SDC are protected with physical security and additional PIN/access card-based system for restricted entry and exit. Supplier must ensure CCTV cameras cover SDC entry and exit zones with CCTV recordings for at least 90 days, and entry and exit logs (for PIN/access card systems) maintained for at least 3 Years.

4.5.5 Supplier must build opaque enclosures that block visibility from outside the SDC to prevent shoulder-surfing by unauthorized personnel.

4.5.6 Supplier must ensure only named Supplier Personnel assigned to New York Life are permitted to enter the SDC. All other persons (excepting only maintenance and emergency workers such as police, firemen, emergency medical services and similar individuals) require express prior written approval of New York Life before entering any New York Life dedicated areas.

4.5.7 Supplier must ensure that bags and personal devices are not brought into an SDC without express written authorization of New York Life. Unless prohibited by Applicable Law, any permitted bags must be inspected both upon entering and exiting the SDC.

4.5.8 Supplier must enforce a clear desk policy in the SDC and must deploy document shredders (micro-cut, pulverizing, or equally secure) for destroying documents.

4.5.9 Supplier must ensure printers are kept out of the SDC and that printing capabilities from Supplier Systems leveraged by the SDC IT infrastructure is disabled.

4.6 Network & Communications Security

4.6.1 Supplier must ensure that the entire telecommunications and data network for the SDC, including routers, switches, and firewalls, is physically segregated, including separate network equipment and cabling, from Supplier's Internet access demarcation point. Network infrastructure used for the SDC must not be shared with any co-tenants.

4.6.2 Supplier must ensure cables are concealed to prevent accidental or malicious interference and labelled to maintain segregation without drawing attention to the usage.

4.6.3 Supplier must ensure all unused ports are disabled.

4.6.4 Supplier must ensure guest wireless access is disabled inside the SDC.

4.6.5 Supplier must maintain a firewall rule recertification process. Unused or inactive rules should be reviewed and removed at least annually.

4.6.6 Supplier must enable firewall logging for all types of traffic and monitor for any suspicious activity. Firewall logs must be available for review when requested.

4.6.7 Supplier must prohibit access to Supplier email, Instant Messaging (IM), or any other Collaboration/Messaging sites from within the SDC. Supplier must provide details of such tools to be disabled within the SDC.

4.7 Telephony

4.7.1 Supplier must secure all call control elements (PBX) against unauthorized access.

4.7.2 Supplier must ensure voice systems have proper controls that comply with voice recording.

4.7.3 Supplier must not provide Call Detail Records (CDR) to a third-party without prior written authorization from New York Life.

4.8 Infrastructure/Platforms/Services/Desktop/Operations Security

4.8.1 Supplier must ensure only a New York Life certified, secure desktop technology is deployed in the SDC.

4.8.2 Supplier must ensure only New York Life authorized software is installed on desktops in the SDC.

4.8.3 Supplier must ensure that all internet access to the SDC is routed via New York Life proxy servers.

4.8.4 Supplier must ensure Remote Access (from outside the SDC) is prohibited unless approved in advance and in writing by New York Life. All such approvals must be maintained and made available for both Supplier and New York Life audits.

4.8.5 Supplier must ensure administrator-level privileges to Scoped IT Assets are authorized by New York Life and must provide a list of all Supplier Personnel with administrator-level privileges to New York Life on a monthly basis.

4.8.6 Supplier must ensure business continuity plans are reviewed and approved in writing by New York Life on a periodic basis or as requested.

5.0 End Point Security

5.1 Supplier Managed Device(s)

5.1.1 Supplier must ensure that Supplier Managed Devices are leveraged as the preferred means for remote access to Supplier's network, unless business, operational or technological constraints prevents their use. In such cases, Supplier should leverage Supplier provided VDI for remote access to Supplier's network from non-Supplier Managed Devices.

5.1.2 Supplier must ensure that all Supplier Managed Devices adhere to the following:

1. All devices must be domain joined, password protected and require Multi-Factor Authentication (MFA).
2. Local administrator and guest accounts are renamed, and administrative privilege are not granted to End Users.
3. Implement time-out and termination of system communication sessions and security sessions or contexts after fifteen (15) minutes of End User inactivity.
4. Data Loss Protection (DLP) software is installed on the endpoint.
5. Remote connections are required to connect through a secure, always on Virtual Private Network (VPN) client (e.g., Cisco AnyConnect client, Palo Alto Global Protect).
6. VPN profile configurations are configured to disable split tunneling.
7. Full disk encryption is configured on all endpoints using at least a 256 bit encryption (e.g., Microsoft BitLocker).
8. Screen capturing tools (e.g., print screen, screen recording, and snipping tool) are disabled unless approved in writing by New York Life. Approved screen capture access should be monitored using DLP software.

9. Saving data to USB and portable devices is strictly prohibited and must be disabled unless approved in writing by New York Life. Approved USB devices should be encrypted using Approved Encryption.
10. Booting from active devices like CD-ROM, Floppy Drive, Boot ROM, etc. is disabled.
11. Centrally managed malicious control system and endpoint detection and response (EDR) client is deployed, configured, and monitored by the Supplier 24/7 Security Operations Center (SOC) (e.g., Cisco Advanced Malware Protection (AMP)).
12. All security software installed on a Supplier Managed Device is monitored 24x7 for any alerts and actioned for follow up.
13. Group Policy Object (GPO) settings are deployed and configured to harden and manage the device on demand.
14. The Microsoft System Center Configuration Manager (SCCM) client or equivalent is required to allow packages and patches to be pushed out to the device as needed.
15. All remote access to New York Life Data must have printing capabilities disabled.

5.2 Supplier Provided Virtual Desktop Interface (VDI)

5.2.1 Where Supplier provided VDI is the resource, Supplier must implement the following controls:

1. VDI must prohibit screen capture within the VDI guest.
2. VDI must prohibit the mapping, mounting, and sharing of disk drives both internal and external to the guest.
3. VDI must prohibit clipboard access (copy and paste) from the guest to the host.
4. If the provided VDI is Internet facing (publicly accessible), access into the VDI infrastructure must be protected with MFA.
5. VDI solutions must be configured to disable the ability to download New York Life Data to a location outside the New York Life network.

6.0 Glossary

6.1 Access Control

Access Control means to ensure that access to Scoped IT Assets is authorized and restricted based on business and security requirements.

6.2 Accountability

Accountability means responsibility of an entity for its actions and decisions.

6.3 Agreement

Agreement means the written agreement between Supplier and New York Life applicable to Supplier's provision of products and services to New York Life.

6.4 Applicable Law

Applicable Law has the meaning specified in the Agreement.

6.5 Approved Encryption

Approved Encryption means the following standards, as well as any successor industry-accepted encryption method or algorithm that establishes more protective standards or protocols or any other encryption method or algorithm as may be required or requested by New York Life:

a) Encryption algorithms must be industry-accepted and in wide use, tested by multiple independent parties and meet the minimum key lengths defined below.
    1. For symmetric encryption, minimum standard key length of at least 256 bits;
    2. For asymmetric encryption, a minimum standard key length of at least 2048 bits;
    3. Elliptic Curve systems should have 224-bit ECC or higher; or
    4. Hashing algorithms should be SHA2 or SHA256 or better.

b) Data transmission of any New York Life Data over public networks (including the Internet) or wireless networks (including cellular) must be encrypted as follows:
    1. Methods that are approved are SFTP, FTPS, HTTPS, Secure Shell (SSH) 2.0 or later, TLS 1.2 or later, FTP with PGP file encryption, and Virtual Private Network (VPN) (any changes by Supplier to the method or standard of transmission used must be approved in advance by New York Life).
    2. Data transmissions via email will be appropriately encrypted using Transport Layer Security (TLS) 1.2 or later or S/MIME, or another encryption method approved by New York Life's Information Security & Risk Team.
    3. Wireless networks must be encrypted using WiFi Protected Access 2 (WPA2) or later.
    4. Other methods are subject to New York Life Information Security & Risk Team's approval.
    5. All Hardware Security Modules (HSM) must adhere to NIST FIPS 140-2 Security Requirements for Cryptographic Modules standard.

6.6 Availability

Availability means the accessibility and usability of information.

6.7 Confidentiality

Confidentiality generally means the privacy of data; ensures that information is not disclosed to unauthorized persons or processes. The primary methods for achieving confidentiality are authentication, authorization, and encryption. Confidentiality requirements are more specifically set forth in the Agreement.

6.8 End User

End User means, depending on the context, (A) Supplier Personnel, and/or (B) New York Life's directors, officers, employees, agents, auditors, consultants, suppliers, service providers, and contractors.

6.9 Hold Order(s)

A notice issued in connection with litigation and regulatory matters and require the preservation of certain electronic and physical Records and non-records (documents).

6.10 Hosted Services

Hosted Services means that the services provided by a Supplier to New York Life are hosted within, and/or managed from the Supplier's environment, including any related software, applications, databases, websites, servers, Supplier Systems, third party cloud providers, and any other IT equipment and technology.

6.11 Integrity

Integrity means the consistency of data; ensures that an unauthorized person or system cannot inadvertently or intentionally alter data.

6.12 High Risk Transaction

A High Risk Transaction is a transaction or client inquiry that poses a high potential for financial or reputational loss to either New York Life or its clients if the transaction is unauthorized and may include:

a) Change of Contact Information

b) Bank Account Change

c) Beneficiary Change

d) Disbursement of any amount or asset (i.e. cash or securities)

e) Request for Policy/Account Number

f) Request for tax forms, account statements, and annual policy summaries

g) Ownership Changes

h) Account Closure Requests

6.13 Least Privilege

Least Privilege means a security practice, similar to need-to-know, that requires minimal access to all data, applications, systems and networks in a computing environment. End Users (including service or support accounts), applications and systems must be able to access only the information and resources that are necessary for its legitimate purpose.

6.14 Multi-Factor Authentication

Multi-Factor Authentication means provision of assurance that a claimed characteristic of an entity is correct through the verification of at least two of the following types of factors:

a) Something a person knows (Knowledge Factor) – This represents information of which only the legitimate user should have knowledge (e.g., a password). Often referred to as basic authentication.

b) Something the person has (Possession Factor) – This represents a physical object, which is not trivial to the duplicate, over which only the legitimate user has possession and control (e.g. hardware token physical access to a protected location, etc.).

c) Something a person is (Inherence Factor) – This is using unique physical traits of an individual such as iris or fingerprint, which cannot be duplicated on another individual.

6.15 New York Life

New York Life means (A) New York Life Insurance Company, (B) any entity that directly or indirectly controls, is controlled by, or is under common control with New York Life Insurance Company, and (C) its and their respective directors, officers, employees, agents, auditors, consultants, suppliers, service providers, and contractors (excluding Supplier and Supplier Personnel).

6.16 New York Life Data

New York Life Data means: New York Life's Confidential Information and NYL Materials (as each term is specified in the Agreement or, if not specified in the Agreement, as defined in New York Life's Supplemental Glossary for Supplier Security Standard).

6.17 Service Delivery Center (SDC)

Service Delivery Center (SDC) means all or a portion of an on-shore, near-shore, or off-shore facility, from or through which Supplier Personnel provide services to New York Life, or have access to Scoped IT Assets, New York Life Data (excluding public data), systems, hardware, or software and which is solely dedicated to supporting NYL.

6.18 Non-Dedicated SDC

A Non-Dedicated SDC means all or a portion of a facility that is not solely dedicated to performing New York Life services, and the technology infrastructure (i.e. firewalls, routers, etc.) may not be solely dedicated to New York Life.

6.19 Dedicated SDC

A Dedicated SDC means all or a portion of a facility that is solely dedicated to New York Life, where the SDC technology infrastructure (e.g., servers & network equipment) is dedicated to New York Life; is distinct and segregated from co-tenants and is subject to a formal documented auditable process to ensure appropriate management of access.

6.20 SDC Supplier

SDC Supplier means a Supplier that provides services to New York Life via a Service Delivery Center.

6.21 Record(s)

Information that must be retained due to legal or regulatory requirements or because they capture significant business activity, regardless of the format (e.g., electronic or physical)

6.22 Risk-Based Authentication

Risk-Based Authentication means authentication that detects anomalies or changes in the normal use patterns of an Account and requires additional verification of the person's identity when such deviations or changes are detected, such as through the use of challenge questions.

6.23 Scoped IT Asset

Scoped IT Asset means (A) Supplier Systems, and (B) New York Life Data.

6.24 Security Event

Security Event has the meaning specified in the Agreement.

6.25 Subcontractor

Subcontractor has the meaning specified in the Agreement.

6.26 Supplier

Supplier means the counterparty to New York Life in the Agreement.

6.27 Supplier Managed Device(s)

Supplier Managed Device(s) are endpoint devices that are managed by the supplier including device configurations and security settings. Managed Devices include, but are not limited to laptops, desktops, tablets and mobile phones.

6.28 Supplier Personnel

Supplier Personnel has the meaning specified in the Agreement.

6.29 Supplier Systems

Supplier's Systems has the meaning specified in the Agreement.

6.30 Vulnerability

Vulnerability means weakness of a Scoped IT Asset or control that can be exploited by a threat.